

GeekBrains

Урок 2 Видео 4

Криптография

Byte-at-a-time ECB decryption

В этом видео

1. Пример уязвимой схемы, построенной на основе ECB
2. Эксплуатация уязвимой схемы

???-???-ECB(input || secret, key)

Если злоумышленник может контролировать значение “input”, то он может узнать “secret”.



Шаги для эксплуатации

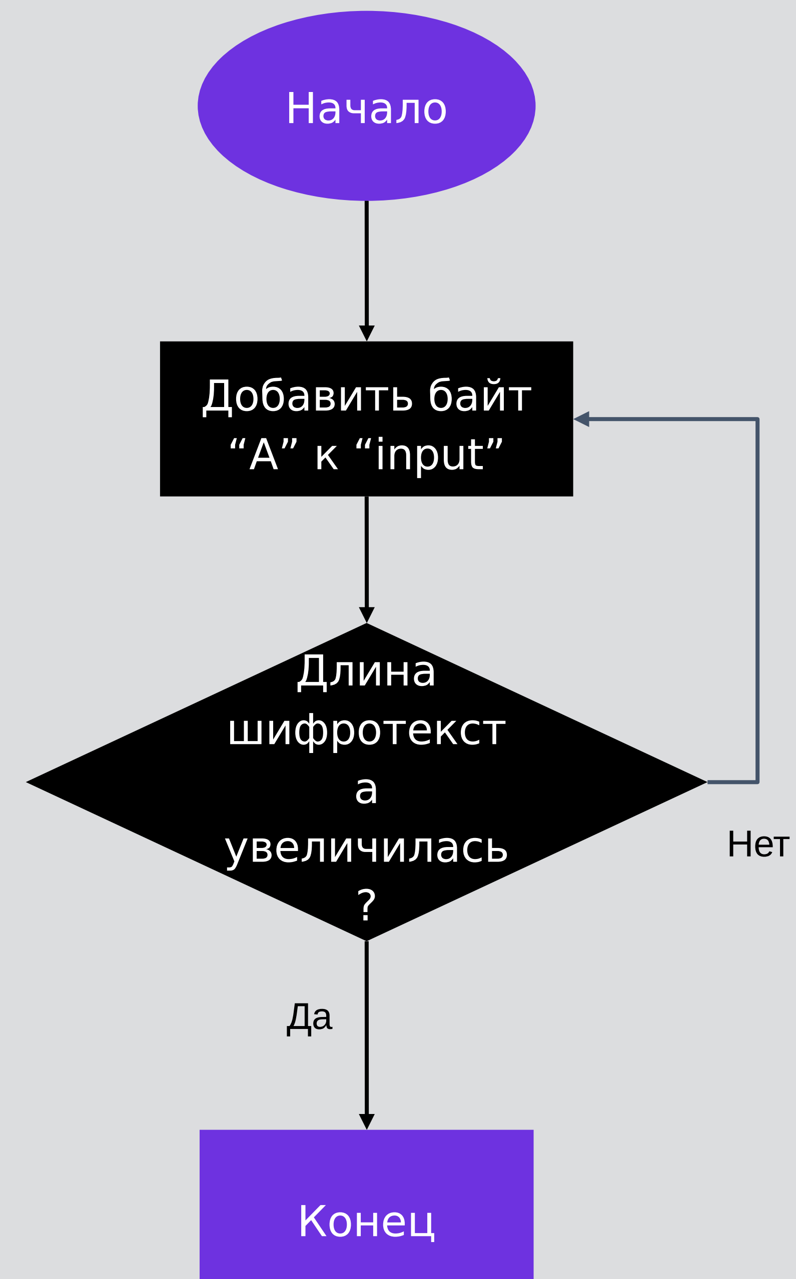
Определить размер блока

Определить используется ли ECB режим

По байтику, по байтику...

GeekBrains

Как узнать длину блока?



AES-64-ECB(input || secret, key)

4141414141414141 ???????????????? ... => ea0b342957394717 d1f5023034147465

AES-64-ECB(input || secret, key)

4141414141414141 ???????????????? ... => ea0b342957394717 d1f5023034147465

41414141414141?? ???????????????? ... => 4e2827f25a08fb40 d1f5023034147465

AES-64-ECB(input || secret, key)

4141414141414141 ???????????????? ... => ea0b342957394717 d1f5023034147465

41414141414141?? ???????????????? ... => 4e2827f25a08fb40 d1f5023034147465

41414141414141**00** => **31e63b5e0f00175c**

AES-64-ECB(input || secret, key)

4141414141414141 ???????????????? ... => ea0b342957394717 d1f5023034147465

41414141414141?? ???????????????? ... => 4e2827f25a08fb40 d1f5023034147465

4141414141414100 => 31e63b5e0f00175c
4141414141414101 => 07385432442 1e6f9

AES-64-ECB(input || secret, key)

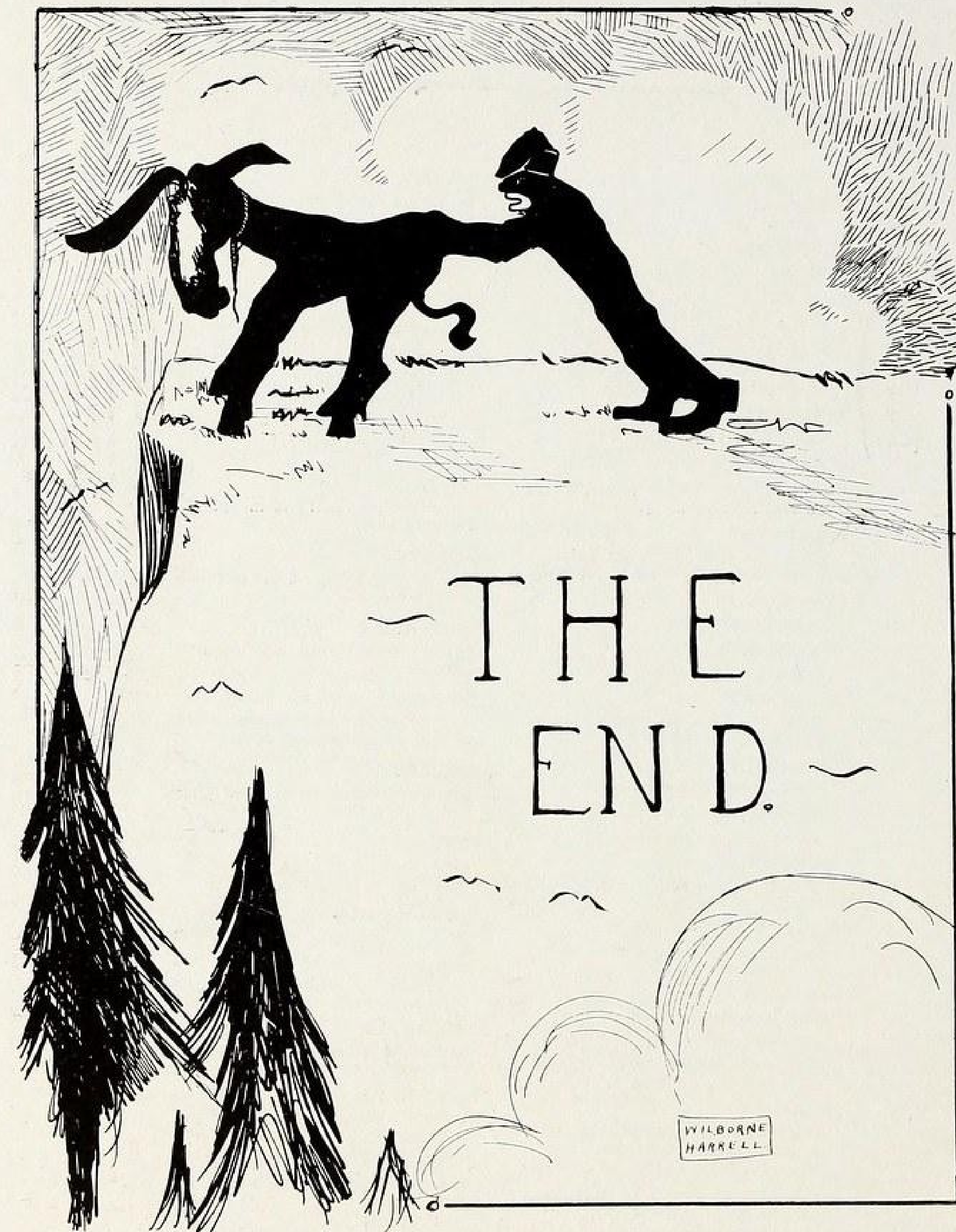
4141414141414141 ???????????????? ... => ea0b342957394717
d1f5023034147465

41414141414141?? ???????????????? ... => 4e2827f25a08fb40
d1f5023034147465

4141414141414100 => 31e63b5e0f00175c
4141414141414101 => 073854324421e6f9
4141414141414102 => 27383e271212191f
...
4141414141414157 => 4e2827f25a08fb40

GeekBrains

Первый байт (0x57, ascii W) мы подобрали. Похожим образом подбираются все оставшиеся байты “secret”-а.



Итоги

1. Увидели пример уязвимой схемы
2. Научились эксплуатировать уязвимую схему ECB